Docket No. 99-064 MIS

CLAIMS:

What is claimed is:

1   1.   An encryption key management system comprising:

2   a master key; and

3   a portable processor, wherein the portable

4   processor uses the master key for generating an

5   encryption key.

1   2.   The encryption key management system recited in claim

2   1 further comprising:

3   a variable key range variable, wherein the

4   portable processor further uses the variable key range

5   variable for generating the encryption key.

1   3.   The encryption key management system recited in claim

2   2, wherein the variable key range variable is output with

3   the encryption key.

1   4.   The encryption key management system recited in claim

2   2, wherein the variable key range variable comprises at

3   least one of a card number, a card group number and a

4   reference number representing a number of keys.

1   5.   The encryption key management system recited in claim

2   2, wherein the portable processor further comprises:

3   a hashing function for generating the encryption

4   key.

Docket No. 99-064 MIS

1 6.   The encryption key management system recited in claim

2 1, wherein the portable processor is a smart card.

1 7.   The encryption key management system recited in claim

2 6, wherein the smart card is accessed through verification

3 of a personal identification number.

1 8.   The encryption key management system recited in claim

2 4, wherein the portable processor further comprises:

3   an incrementor for increasing the value of the

4   reference number in response to the encryption key

5   being generated.

1 9.   The encryption key management system recited in claim

2 1, wherein the portable processor is a first portable

3 processor and the system further comprises:

4   a second portable processor, wherein the portable

5   processor uses the master key for generating a

6   decryption key.

1 10.   The encryption key management system recited in claim

2 9, wherein the second portable processor further uses the

3 variable key range variable for generating the encryption

4 key.

1 11.   The encryption key management system recited in claim

2 10, wherein the variable key range variable is input to the

3 second portable processor.

Docket No. 99-064 MIS

1 12.   The encryption key management system recited in claim
2 10, wherein the second portable processor further
3 comprises:
4   a hashing function for generating the decryption
5   key using the master key.

1 13.   The encryption key management system recited in claim
2 9, wherein the second portable processor is a smart card.

1 14.   The encryption key management system recited in claim
2 13, wherein the smart card is accessed through verification
3 of a personal identification number.

1 15.   The encryption key management system recited in claim
2 10, wherein the second portable processor further
3 comprises:
4   a hashing function for generating the decryption
5   key.

1 16.   An encryption key management system comprising:
2   a master key; and
3   a portable processor, wherein the portable
4   processor uses the master key for generating a
5   decryption key.

1 17.   The encryption key management system recited in claim
2 16 further comprising:
3   a variable key range variable, wherein the
4   portable processor further uses the variable key range
5   variable for generating the decryption key.

Docket No. 99-064 MIS

18. The encryption key management system recited in claim
17, wherein the variable key range variable is output with
the decryption key.

19. The encryption key management system recited in claim
16, wherein the variable key range variable comprises at
least one of a card number, a card group number, and a
reference number representing a number of keys.

20. The encryption key management system recited in claim
17, wherein the portable processor further comprises:
        a hashing function for generating the decryption
key.

21. The encryption key management system recited in claim
16, wherein the portable processor is a smart card.

22. An encryption key management method comprising:
        receiving a master key;
        generating an encryption key using the master
key, wherein the encryption key is generated by a
portable processor; and
        outputting the encryption key.

23. The method recited in claim 22 prior to generating an
encryption key the method further comprises:
        creating a variable key range variable, wherein
the portable processor uses the variable key range
variable for generating the encryption key.

Docket No. 99-064 MIS

1   24.   The method recited in claim 23 further comprises:

2   outputting the variable key range variable.

1   25.   The method recited in claim 23, wherein the variable

2   key range variable comprises at least one of a card number,

3   a card group number, and a reference number representing a

4   number of keys.

1   26.   The method recited in claim 23, wherein generating the

2   encryption key further comprises:

3   hashing the master key.

1   27.   The method recited in claim 23, wherein the portable

2   processor is a smart card.

1   28.   The method recited in claim 27 further comprises:

2   verifying a personal identification number; and

3   accessing functionality of the smart card.

1   29.   The method recited in claim 22, wherein the portable

2   processor is a first portable processor and the method

3   further comprises:

4   generating a decryption key using the master key,

5   wherein the decryption key is generated by a second

6   portable processor; and

7   outputting the decryption key.

1   30.   The method recited in claim 29, prior to generating

2   the encryption key further comprises:

Docket No. 99-064 MIS

3   receiving a variable key range variable, wherein

4   the second portable processor uses the variable key

5   range variable for generating the encryption key.

1   31.   The method recited in claim 23, wherein the second

2   portable processor is a smart card.

1   32.   The method recited in claim 22, wherein a smart card

2   is accessed through verification of a personal

3   identification number.

1   33.   An encryption key management method comprising:

2   receiving a master key; and

3   generating a decryption key using the master key,

4   wherein the decryption key is generated by a portable

5   processor; and

6   outputting the decryption key.

1   34.   The method recited in claim 33 prior to generating the

2   decryption key the method further comprises:

3   creating a variable key range variable, wherein

4   the portable processor uses the variable key range

5   variable for generating the decryption key.

1   35.   The method recited in claim 34 further comprises:

2   outputting the variable key range variable.

1   36.   The method recited in claim 34, wherein the variable

2   key range variable comprises at least one of a card number,

Docket No. 99-064 MIS

3   a card group number, and a reference number representing a

4   number of keys.

1   37. The method recited in claim 34, wherein generating the

2   decryption key further comprises:

3   hashing the master key.

1   38.   The method recited in claim 34, wherein the portable

2   processor is a smart card.